

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN RE: BON SECOURS MERCY
HEALTH DATA BREACH
LITIGATION

Case No. 1:24-cv-594

JUDGE DOUGLAS R. COLE

OPINION AND ORDER

Plaintiffs Alison Lausche, Sarah Speights, and LaTisha Smalls bring this putative class action against Defendant Bon Secours Mercy Health, Inc. (Bon Secours) based on what they say was a preventable data breach of Bon Secours' inadequately protected computer network. Bon Secours now moves to dismiss for lack of standing and failure to state a claim. Ultimately, the Court concludes that Plaintiffs have standing for most of their claims and allege facts that plausibly support some of the claims as to which they have standing. The Court therefore **GRANTS IN PART** and **DENIES IN PART** Bon Secours' Motion to Dismiss (Doc. 17).

BACKGROUND¹

Bon Secours is among the nation's twenty largest healthcare systems. (Am. Compl., Doc. 13, #92). It operates 48 hospitals across seven states and has over 60,000 employees. (*Id.*). When Bon Secours hires a new employee, it requires that individual

¹ As this matter is before the Court on Bon Secours' motion to dismiss, the Court generally must accept the well-pleaded allegations in the Amended Complaint as true. *Bassett v. Nat'l Collegiate Athletic Ass'n*, 528 F.3d 426, 430 (6th Cir. 2008). But the Court reminds the reader that they are just that—allegations.

to turn over various personally identifiable information (PII), which it then stores on its computer network. (*Id.* at #92, 104, 106, 109).

Unfortunately, in 2024, Bon Secours detected “suspicious activity” on a portion of that computer network—more specifically, its “Workday test environment.” (*Id.* at #96). So it launched an investigation. That investigation revealed that, between April 10, 2024, and July 31, 2024, unknown bad actors had gained unauthorized access to various data files Bon Secours housed on the network. (*Id.* at #96–97). Plaintiffs allege that the breach compromised thousands of individuals’ “names, dates of birth, Social Security numbers, addresses, and other demographic information,” including theirs. (*Id.* at #97). And according to Plaintiffs, Bon Secours did not notify affected individuals of the data breach until “several weeks” after learning about it, which “further exacerbated” Plaintiffs’ and putative class members’ harms. (*Id.*). The notice that Bon Secours ultimately sent to affected individuals, though, was careful to state that the company, based on its investigation, was “not aware of [PII] being misused” and that it was making potentially affected individuals “aware out of an abundance of caution.” (Doc. 17-1, #192).

Plaintiffs, however, are not convinced. Start with Lausche. She is an Ohio resident, who, like Speights and Smalls, provided her PII to Bon Secours “in exchange for” employment. (Doc. 13, #94, 104, 106, 109). She received a notice from Bon Secours that her PII, including her social security number, had been exposed in the data breach. (*Id.* at #104). Lausche claims that she is “very careful” about sharing her personal information and that, to her knowledge, she has not had her PII exposed in

any data breaches before this one. (*Id.*). Since this breach, however, Lausche has experienced a substantial uptick in the number of spam phone calls and texts she receives. (*Id.* at #105). And she's spent significant time attempting to mitigate the effects of the breach, such as reviewing her accounts and taking steps to protect her data from future harm. (*Id.*). Indeed, the notice Bon Secours sent her apparently instructed Lausche to remain "vigilant" by reviewing account statements and credit reports for signs of identity theft or fraud. (*Id.*). Because of all that, Lausche has experienced stress, anxiety, and concern about the consequences of bad actors accessing her PII. (*Id.* at #105–06).

Speights's allegations tell a similar story. She is a Virginia resident who also handed over her PII to Bon Secours in exchange for employment. (*Id.* at #94, 106). And like Lausche, Speights alleges she has always been careful about sharing her PII and has not had any information divulged in a breach before this one, at least to her knowledge. (*Id.* at #107). Since this data breach, though, Speights alleges that she's been the victim of identity theft. (*Id.* at #106–07). Specifically, she points to \$1,100 of unauthorized transactions on her financial account, which she says occurred in the months following the data breach. (*Id.* at #107). So she's spent numerous hours trying to address that issue, disputing the transactions with her bank, locking the account, and changing passwords. (*Id.* at #107–08). And Speights, in accordance with Bon Secours' notice letter's instructions, has spent additional time seeking to prevent future incidences of identity theft. (*Id.* at #108). Stress, anxiety, and concern have plagued Speights as a result of the identify theft. (*Id.*).

That leaves Smalls, whose allegations largely mirror the other two Plaintiffs'. She is a South Carolina resident who, in exchange for employment, provided Bon Secours' her PII. (*Id.* at #94, 109). Smalls has been similarly careful with her personal information, which, to her knowledge, hasn't been the subject of a data breach before this one. (*Id.* at #109). Because of this data breach, Smalls—like Speights—has allegedly experienced identity theft. (*Id.* at #110). In November 2024, Smalls was notified that someone has fraudulently opened a credit account in her name, which, in turn, negatively impacted her credit and delayed her in efforts to secure an apartment. (*Id.*). And Smalls—like Lausche—has also noticed an upswing in the number of spam calls and texts she's receiving since the data breach. (*Id.*). So she's spent substantial time attempting to ameliorate the fraudulent credit card situation and trying to avoid future issues. (*Id.* at #110–11). As with the notices the other Plaintiffs received, Smalls' notice from Bon Secours instructed her to “remain vigilant” of identity theft and fraud. (*Id.* at #111). In sum, Smalls has experienced stress, anxiety, worry, and concern because of the breach and its consequences. (*Id.*).

All told, Plaintiffs collectively allege that Bon Secours had an obligation to protect their PII but negligently did so by failing to use adequate data security measures. (*Id.* at #112–14). And they say that Bon Secours' failure to thwart a preventable and foreseeable data incident breached the express and implied contracts Plaintiffs held with Bon Secours. (*Id.* at #119–22). They claim that cybercriminals will exploit (or already have exploited) the divulged data to commit identity theft and fraud, especially given the availability of “Fullz” packages—dossiers of information

unauthorized parties can assemble by cross-referencing PII compromised in a data breach with publicly available data. (*Id.* at #100, 114–19).

Based on those allegations Plaintiffs assert five claims: (1) negligence (Count I); (2) breach of express contract (Count II); (3) breach of implied contract (Count III); (4) unjust enrichment (Count IV); and (5) a claim for declaratory judgment and injunctive relief (Count V). (*Id.* at #125–40). And they seek to certify a nationwide class of “[a]ll persons residing in the United States whose Personal Information was compromised as a result of the Data Breach.” (*Id.* at #122).

Bon Secours now moves to dismiss Plaintiffs’ Amended Complaint for two reasons. First, it claims Plaintiffs lack standing and thus that the Court lacks jurisdiction. Specifically, Bon Secours complains that: (1) Plaintiffs did not allege actual or imminent injuries sufficient to confer Article III standing, and (2) even if they did, those injuries are not traceable to the data breach. (Doc. 17, #172–82). Second, Bon Secours argues that, even if Plaintiffs have standing, they did not plausibly allege their various claims. (*Id.* at #182–88).

Plaintiffs responded, arguing essentially the opposite, (*see generally* Doc. 18), and Bon Secours replied, (Doc. 20). So the motion is now ripe.

LEGAL STANDARD

Bon Secours moves to dismiss this action under both Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Ultimately, the standard the Court employs to analyze each is “similar,” *Ohio Nat. Life Ins. Co. v. United States*, 922 F.2d 320, 325 (6th Cir. 1990), though they remain separate inquiries.

Start with the former. A motion challenging standing (and thus the Court's subject-matter jurisdiction) under Federal Rule of Civil Procedure 12(b)(1) can mount either a facial attack or a factual one. *Ohio Nat.*, 922 F.2d at 325. Bon Secours here asserts a facial attack, (Doc. 17, #171), which “merely questions the sufficiency” of the Amended Complaint, *Ohio Nat.*, 922 F.2d at 325. So in reviewing the motion, the Court “must accept all allegations as true,” except that it need not credit “[c]onclusory allegations or legal conclusions masquerading as factual conclusions.” *Rote v. Zel Custom Mfg. LLC*, 816 F.3d 383, 387 (6th Cir. 2016) (quotation omitted). Then, having done so, the question is whether those allegations are sufficient on their face to “establish federal claims.” *Id.* If they are, then the Court may properly exercise subject-matter jurisdiction. *Id.*

Now consider the latter. To survive a motion to dismiss under Rule 12(b)(6), Plaintiffs must allege “sufficient factual matter ... to state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (cleaned up). While a “plausible” claim for relief does not require a showing of *probable* liability, it requires more than “a sheer possibility that a defendant has acted unlawfully.” *Iqbal*, 556 U.S. at 678 (citation omitted). The Amended Complaint must allege sufficient facts that allows the Court to “draw the reasonable inference that the defendant is liable.” *Id.* And at the motion-to-dismiss stage, the Court accepts the facts of the Amended Complaint as true. *Id.* But that does not mean the Court must take everything Plaintiffs allege as gospel, no matter how far-fetched. The Court may

disregard “naked assertions” of fact or “formulaic recitations of the elements of a cause of action.” *Id.* (cleaned up).

LAW AND ANALYSIS

Before turning to the standing and merits analyses, the Court first notes that it has subject-matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), (5). That is so because the parties are at least minimally diverse,² the putative class exceeds 100 members, and the amount in controversy purportedly exceeds \$5,000,000. Moreover, venue is proper because Bon Secours resides here—its principal place of business is in Cincinnati, Ohio. 28 U.S.C. § 1391(b)(1). With that out of the way, the Court turns to whether Plaintiffs have standing to sue. They do—at least for most of their claims. So the Court also addresses the sufficiency of those claims, and ultimately concludes that most pass the *Iqbal/Twombly* threshold.

A. Plaintiffs Have Article III Standing to Pursue Damages and Certain Injunctive Relief.

1. Plaintiffs Have Standing to Pursue Damages.

Article III § 2 of the Constitution limits a federal court’s jurisdiction to “cases” and “controversies.” A plaintiff’s standing to sue is one element of this constitutional requirement. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 422–23 (2021). To have standing, a plaintiff must show that: (1) she suffered a concrete, particularized, and

² Minimal diversity requires that at least one plaintiff is diverse from at least one defendant. *Life of the S. Ins. Co. v. Carzell*, 851 F.3d 1341, 1344 (11th Cir. 2017) (citing 28 U.S.C. § 1332(d)(2)(A)). Here, Plaintiffs are citizens of Ohio, Virginia, and South Carolina. (Doc. 13, #94). And Bon Secours, according to the Complaint, is a Maryland company with a principal place of business in Cincinnati, Ohio. (*Id.* at #95). Minimal diversity is therefore satisfied.

actual or imminent injury; (2) the injury is traceable to the defendant’s conduct; and (3) a favorable ruling would redress that injury. *Id.* at 423. Bon Secours here challenges Plaintiffs’ standing on the first two elements: injury and traceability. (Doc. 17, #172–82). So the Court addresses each in turn.

Start with injury. As noted, “[u]nder constitutional standing doctrine, an ‘injury in fact’ is an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical.” *Merck v. Walmart, Inc.*, 114 F.4th 762, 773 (6th Cir. 2024) (cleaned up). A plaintiff can satisfy that two-part requirement in a variety of ways. First, a plaintiff can rely on *actual* harms. “[I]f the plaintiff suffers an actual (i.e., presently occurring) tangible harm, like physical injury or economic loss,” that satisfies the injury-in-fact requirement. *Savidge v. Pharm-Save, Inc.*, 727 F. Supp. 3d 661, 681 (W.D. Ky. 2024) (citing *TransUnion*, 594 U.S. at 425). Or if a plaintiff “suffers an actual (i.e., presently occurring) intangible harm, like reputational harm, for which there is a close historical or common-law analog,” that also works. *Id.* (citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340–41 (2016)).

Beyond *actual* harms, a plaintiff can also rely on a risk of future harm to meet his or her burden. That future harm, however, must be both sufficiently imminent and concrete to qualify as an injury. *Id.* (citing *TransUnion*, 594 U.S. at 437–38; *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 415 (2013)). In data breach cases, courts often look to “the three non-exhaustive *McMorris* factors to determine if the risk of harm” refers to harm that is sufficiently imminent. *Id.*; see also *McMorris v. Carlos*

Lopez & Assocs., LLC, 995 F.3d 295, 301–02 (2d Cir. 2021). “Then, to satisfy the concreteness requirement, the future harm must have a close relationship to a harm traditionally recognized” at common law. *Savidge*, 727 F. Supp. 3d at 681–82 (citing *TransUnion*, 594 U.S. at 424). And in damages suits, a plaintiff must show that “the risk of future harm materialized” or that she was “independently harmed by [her] exposure to the risk itself.” *Ward v. Nat’l Patient Acct. Servs. Sols., Inc.*, 9 F.4th 357, 361 (6th Cir. 2021).

Bon Secours says that Plaintiffs cannot establish an injury-in-fact under any of those iterations because they have pleaded neither an actual injury, nor a risk of an imminent one. (Doc. 17, #172–82). Plaintiffs counter that they’ve pleaded both kinds of injury, firing off various theories in support: (1) theft of their valuable PII; (2) imminent and certainly impending injury from fraud and identity theft; (3) invasion of privacy; (4) breach of confidentiality; (5) diminution in value of their PII; (6) lost benefit of their bargain with Bon Secours; and (7) time and expenses incurred mitigating the actual and potential impact of the breach. (Doc. 18, #210). Ultimately, the Court concludes that each Plaintiff has alleged an already-incurred actual injury—either identity theft and fraud or spam and harassment—sufficient to confer Article III standing. So the Court need not address the various other theories Plaintiffs present.³

³ Because each of Plaintiffs’ claims arise from the same data breach and neither Plaintiffs nor Bon Secours argues that the standing inquiry differs among the various claims, the Court will treat the damages claims together throughout its analysis. *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 373 n.3 (1st Cir. 2023).

Two Plaintiffs—Speights and Smalls—allege facts plausibly suggesting that they have experienced identity theft because of the data breach. Speights points to unauthorized transactions to the tune of \$1,100 that have occurred on her financial account in the months following the data breach. (Doc. 13, #107). And Smalls claims that someone opened a fraudulent credit card in her name after the breach. (*Id.* at #110). That sort of actual misuse of a plaintiff’s PII (if that is indeed what happened here) qualifies as a concrete injury. *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 373 (1st Cir. 2023); *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262–63 (11th Cir. 2021); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017).

And Lausche (along with Smalls) alleges that she has started receiving an increased number of spam emails and texts. (Doc. 13, #105, 110). The Court has previously determined that “unsolicited calls and messages constitute cognizable Article III injuries in fact,” even if only by a thin margin. *Tate v. EyeMed Vision Care, LLC*, No. 1:21-cv-36, 2023 WL 6383467, at *5 (S.D. Ohio Sept. 29, 2023) (citing *Dickson v. Direct Energy, LP*, 69 F.4th 338, 345 (6th Cir. 2023)).

In short, both the identity theft and the spam emails and texts “count” as injuries for standing purposes.

Alleging an injury-in-fact, however, isn’t Plaintiffs’ only hurdle. They must also allege causation. On that front, Speights, Smalls, and Lausche alike allege that they are “very careful about sharing [their] sensitive information.” (Doc. 13, #104, 107, 109). And they each attribute the harm they incurred—unauthorized transactions,

opening of a fraudulent credit card, and increased spam communications—to the data breach. (*Id.*). Said differently, without expressly alleging that the data breach “caused” their injuries, Plaintiffs claims those injuries are fairly traceable to it. *Tate*, 2023 WL 6383467, at *6 (citing *Parsons v. U.S. Dep’t of Justice*, 801 F.3d 701, 715 (6th Cir. 2015)). That’s a plausible allegation given that Plaintiffs’ names, birthdates, Social Security numbers, and addresses were divulged in the breach. (Doc. 17-1, #192). Even more so in light of Plaintiffs’ allegation that bad actors can utilize Fullz packages—dossiers of information containing individuals’ personal information—to link individuals’ compromised PII with publicly available information and effectuate identity theft, fraud, or spam communications. (Doc. 13, #100). Taken together, it’s at least plausible, which is all that matters for the standing inquiry at this stage, that Plaintiffs’ injuries are sufficiently traceable to the data breach.

That leaves the redressability element, which Plaintiffs likewise satisfy. Plaintiffs’ injuries sound in tort and contract, both of which can be redressed by money damages. In short, Plaintiffs have standing to pursue damages.

Bon Secours disagrees. In doing so, it doesn’t seriously contend that actual misuse of Plaintiffs’ PII would not qualify as an injury-in-fact. Nor could it. As the Court explained (and as one of the cases Bon Secours cites—*In re SAIC Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014)—confirms), actual misuse counts as an injury in fact. Rather, Bon Secours argues that in failing to allege that phone numbers or financial account information were divulged, Plaintiffs have not shown that their injuries—increased spam calls and unauthorized account

transactions—are traceable to the data breach. (Doc. 17, #176). But that argument fails to persuade.

The very cases Bon Secours cites demonstrate why that is so. In *In re SAIC*, for example, the court noted that a bad actor could obtain certain pieces of PII from a data breach “and then go ‘phishing’ to get the rest,” which might render an unauthorized financial transaction traceable to a data breach even where no bank account data was divulged. 45 F. Supp. 3d at 31. But there, since the plaintiffs did “not allege[] any phishing” or other “plausible explanation for how the thief would have acquired their banking information,” the court found traceability lacking. *Id.* at 31–32. Not so here. Plaintiffs bridge the gap between the type of PII accessed through the breach and the injuries they suffered by alleging the availability of Fullz packages. That is, Plaintiffs say that bad actors used the PII divulged in the data breach, in combination with the Fullz packages, to “link[] to” their phone numbers and other information, which explains how their injuries trace back to the data breach. (Doc. 13, #100). That’s sufficient to plausibly allege traceability.

True, Bon Secours also relies on *Doe v. Mission Essential Group, LLC*, which discounts Fullz packages as a way to establish traceability where the injury at issue is increased spam emails. No. 2:23-cv-3365, 2024 WL 3877530, at *7 (S.D. Ohio Aug. 20, 2024), *appeal dismissed*, No. 24-3815, 2024 WL 5165129 (6th Cir. Dec. 2, 2024). But there are some important differences between that case and this one. In *Doe*, the only PII specifically mentioned was names and social security numbers. *Id.* at *1. Here, there were allegedly additional pieces of information (including addresses and

dates of birth) that bad actors could use to link up the PII with the owner. (Doc. 13, #93). And there, the only injury the court found the plaintiff had plausibly alleged was spam emails, *Doe*, 2024 WL 3877530, at *5–6, while here at least two Plaintiffs have plausibly alleged actual fraudulent transactions, in addition to spam emails.

Against that backdrop, the Court also remains cognizant that “commonsense principles and [a] lax evidentiary standard [] apply at the motion-to-dismiss stage.” *Tate*, 2023 WL 6383467, at *6. Said differently, “Plaintiffs need not *prove* that the data breach caused the increase in scam calls” or unauthorized financial transactions. *Id.* (emphasis in original). “They need only *plausibly allege* that that is the case.” *Id.* (emphasis added). Here, the combination of highly sensitive information (like Social Security numbers, coupled with names, addresses, and dates of birth) being accessed in the data breach, coupled with the opportunity for bad actors to use that information to obtain less sensitive information (like phone numbers), makes it more than a “sheer possibility” that Plaintiffs’ injuries are traceable to the data breach. *Iqbal*, 556 U.S. at 678.

2. Plaintiffs Have Standing to Seek Certain Injunctive Relief, But Not Declaratory Relief.⁴

Beyond damages, Plaintiffs also request declaratory and injunctive relief. (Doc. 13, #137–40). But because “[s]tanding is not dispensed in gross,” Plaintiffs must

⁴ The parties did not address Plaintiffs’ standing to seek declaratory and injunctive relief head-on in their briefing. Regardless, the Court can raise issues of standing sua sponte. *Loren v. Blue Cross & Blue Shield of Mich.*, 505 F.3d 598, 607 (6th Cir. 2007).

separately demonstrate standing for those forms of relief. *TransUnion*, 594 U.S. at 431. Ultimately, they haven't, save for one type of injunctive relief.

Plaintiffs request an injunction requiring Bon Secours to (1) “employ adequate security practices;” (2) “submit to future annual audits of those systems and monitoring procedures;” and (3) “provide Plaintiffs and Class Members with adequate credit monitoring and identity theft restoration services.” (Doc. 13, #139). But the first two of those “forward-looking preventative remedies will do nothing to redress” the “already-occurred injury” of unauthorized access to Plaintiffs’ PII. *Bowles v. Whitmer*, 120 F.4th 1304, 1311 (6th Cir. 2024), *reh’g en banc denied*, No. 24-1013, 2024 WL 5074703 (6th Cir. Dec. 10, 2024). In other words, Plaintiffs have not sufficiently pleaded that *another data breach* is “imminent,” which is necessary to justify an injunction of the type Plaintiffs request. *Mikel v. Quin*, 58 F.4th 252, 258 (6th Cir. 2023), *cert. denied sub nom.*, *Mikel v. Nichols*, 143 S. Ct. 2660 (2023). True, they pleaded that they’re at an imminent risk of identity theft, (*see, e.g.*, Doc. 13, #94), but that’s based on the data breach *that already occurred*. So an injunction requiring Bon Secours to change its security practices or submit to future annual audits “cannot protect the plaintiffs from future misuse of their PII by the individuals they allege now possess it. Any such relief would safeguard only against a future breach.” *Webb*, 72 F.4th at 378. And while Plaintiffs conclusorily pleaded that “[t]he risk of another such breach is real, immediate, and substantial,” (Doc. 13, #139), they offered no *facts* suggesting another breach of Bon Secours’ platform is imminent. Indeed, the Court

finds it unreasonable to infer that Bon Secours faces a higher risk of a future cyberattack than “virtually every holder of private data.” *Webb*, 72 F.4th at 378.

Admittedly, the third version of injunctive relief Plaintiffs seek—requiring Bon Secours to provide them with credit monitoring and identity theft protection for life—could perhaps redress, to some extent, the imminent risk of identity theft that they face because of the already-occurred data breach. The Court is thus satisfied that Plaintiffs have standing to seek this type of injunctive relief alone.⁵

But when it comes to declaratory relief, Plaintiffs once again lack standing. Federal courts may only issue declaratory judgments that have a “conclusive character.” *Mikel*, 58 F.4th at 259 (quoting *Aetna Life Ins. Co. of Hartford v. Haworth*, 300 U.S. 227, 241 (1937)). In other words, a declaratory judgment “may issue only when ‘it is substantially likely’ to redress a plaintiff’s actual or imminent injuries.” *Id.* (quoting *Franklin v. Massachusetts*, 505 U.S. 788, 803 (1992)). But the two declaratory judgments Plaintiffs seek—one announcing that Bon Secours’ existing security measures are not up to snuff and another directing Bon Secours to implement and maintain various security measures, (Doc. 13, #137–38)—are not

⁵ The Court notes that Bon Secours is seemingly already providing the relief Plaintiffs seek. In the notice Bon Secours sent Plaintiffs to inform them of the breach, Bon Secours assured recipients of the following: “[W]e are offering you a complimentary membership in Experian® IdentityWorksSM Credit 3B[, which] helps detect possible misuse of your personal information[, and] provides you with identity protection support[, including] resolution of identity theft.” (Doc. 17-1, #192). If that’s true, an injunction requiring the same would redress nothing. That said, it’s unclear how long that complimentary membership will last. Given that Plaintiffs request an injunction requiring Bon Secours to “provide Plaintiffs and Class Members with adequate credit monitoring and identity theft restoration services for the rest of their lives,” (Doc. 13, #139), the Court is satisfied, at least for present purposes, that an injunction could redress Plaintiffs’ injuries.

conclusive in that sense. Neither declaration would redress the imminent harm arising from bad actors—who currently possess Plaintiffs’ PII—misusing it. Those declarations would at most potentially ameliorate the imminence of a future breach. But, as explained, there’s simply no reason to believe that Bon Secours faces a higher risk of a data breach than any other entity possessing private data.

All told, Plaintiffs lack standing to assert their claim for injunctive relief (except as to credit monitoring and identity theft protection) and declaratory relief. But since they do have standing to bring their claims for damages and for one form of injunctive relief, the Court now turns to the merits of those claims.

B. Plaintiffs Have Plausibly Alleged Their Negligence and Breach of Implied Contract Claims.

Plaintiffs allege negligence, breach of express contract, breach of implied contract, and unjust enrichment. But before considering those claims, a brief choice-of-law analysis is in order. When considering cases arising under a court’s diversity jurisdiction, federal courts apply the choice-of-law rules of the forum state—here, Ohio. *Muncie Power Prods., Inc. v. United Techs. Auto., Inc.*, 328 F.3d 870, 873 (6th Cir. 2003). For tort actions, Ohio choice-of-law follows the Restatement of the Law of Conflicts, which turns on which state possesses the most significant relationship to the tort injury. *Morgan v. Biro Mfg. Co., Inc.*, 474 N.E.2d 286, 289 (Ohio 1984). Factors relevant to the significant relationship test include the place of injury, the residence of the parties, and the place where the relationship of the parties is centered. *Id.* For contract actions, the test is the same, where the factors bearing on the “most significant relationship” include the place of contracting and negotiation,

the place of performance, the location of the subject matter, and the residence of the parties. *Ohayon v. Safeco Ins. Co. of Ill.*, 747 N.E.2d 206, 209 (Ohio 2001).

The Court finds based on the allegations in the Complaint that Ohio has the most significant relationship to this suit. The place-of-injury factor, as the Court has elsewhere explained, doesn't offer much guidance because data breaches are "difficult to 'place' in any physical location." *Tate*, 2023 WL 6383467, at *6. And, while Plaintiffs allege that they entered into contracts with Bon Secours to protect their PII, (Doc. 13, #131–33), that's only marginally helpful because Plaintiffs do not allege the place of contracting, negotiation, or performance for those contracts. Presumably, most of those activities would have occurred at the Bon Secours locations at which each Plaintiff worked. Plaintiffs, however, didn't allege that either. So that leaves the residence of the parties. The named Plaintiffs are scattered across three states—Ohio, Virginia, and South Carolina—and seek to certify a nationwide class, which would presumably increase that count significantly. (*Id.* at #94, 122). The Court therefore finds Bon Secours' residence—and more specifically, its principal place of business, which is Ohio—determinative for present purposes. (Doc. 13, #95). Accordingly, the Court applies Ohio law in assessing the plausibility of the tort and contract actions asserted here.

1. Negligence

A plaintiff alleging negligence must show a duty the defendant owes to the plaintiff, a breach of that duty, and that the breach proximately caused a resulting injury. *Rieger v. Giant Eagle, Inc.*, 138 N.E.3d 1121, 1125 (Ohio 2019).

Plaintiffs here allege that by “accepting and storing” their PII in the course of the employment relationship, Bon Secours incurred both a common-law duty and a statutory duty under the Federal Trade Commission (FTC) Act to safeguard that private information with secure methods. (Doc. 13, #126–27, 130). Plaintiffs claim that Bon Secours breached that duty when it, among other things, failed to utilize adequate security measures to protect the PII. (*Id.* at #127–31). And they add that Bon Secours proximately caused their injuries because a data breach and resultant misuse of exposed PII is the foreseeable consequence of inadequate security measures. (*Id.* at #126, 131).

Bon Secours, in response, argues that Plaintiffs have not sufficiently pleaded the duty and causation elements. As for the former, Bon Secours says there’s no common-law duty for employers to protect employees’ data from third-party cybercriminal attacks, nor does the FTC Act create a private duty to protect that Plaintiffs can enforce. (Doc. 17, #183). Turning to the latter, Bon Secours maintains that Plaintiffs’ failure to allege that their phone numbers or financial information were divulged means they cannot establish that the data breach proximately caused their alleged injuries. (*Id.* at #183–84). And in any event, says Bon Secours, the economic loss rule precludes Plaintiffs from recovering in tort for purely economic loss. (*Id.* at #184).

The Court is ultimately persuaded that Plaintiffs have plausibly alleged their negligence claim. Start with duty. While it is generally the case that there is “no duty to act affirmatively for the protection of others,” certain special relationships impose

a duty to protect. *Jackson v. Forest City Ent., Inc.*, 675 N.E.2d 1356, 1358 (Ohio Ct. App. 1996). “Relationships which result in a duty to protect others include ... employer and employee.” *Id.* (citing Restatement (Second) of Torts § 314 (Am. L. Inst. 1965)). And many courts (although admittedly not the Ohio state courts) have recognized an employer’s duty to protect an employee’s PII in the context of data breaches.⁶ *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 158–59 (3d Cir. 2022); *see also Savidge v. Pharm-Save, Inc.*, No. 3:17-cv-186, 2025 WL 964446, at *8 (W.D. Ky. Mar. 31, 2025) (collecting cases). Plaintiffs here argue that Bon Secours’ purported duty to protect their sensitive data from misuse arises from the employer-employee relationship. (Doc. 13, #104, 106, 109, 125–26). That is enough to plausibly allege a common-law duty to protect.⁷ *Cf. Haney v. Charter Foods N., LLC*, 747 F. Supp. 3d 1093, 1111 (E.D. Tenn. 2024) (applying Tennessee law).

Turn to causation. For the same reasons that Plaintiffs satisfied the traceability element for Article III standing, they likewise exceed the plausibility threshold for the causation element of their negligence claim. That is, even accepting that Plaintiffs’ phone numbers and financial information were not leaked in the data

⁶ Although it doesn’t appear that any Ohio courts have discussed whether an employer has a common-law duty to safeguard employees’ PII, Ohio courts do recognize an employer’s duty to protect its employees when the employer “kn[e]w or should have known that there was a substantial risk of harm to the employees on the premises of the business that are in the possession and control of the owner.” *Smith v. Lincoln Elec. Co.*, 2024-Ohio-5209, ¶ 12 (8th Dist.); *see also Gillotti v. Rimedio*, 2003-Ohio-5708, ¶¶ 27–29 (11th Dist.). That at least hints that Ohio courts would extend an employer’s duty to protect employees to the data breach setting where the employer possesses and controls the employee’s PII.

⁷ Because the Court finds a common-law duty to protect exists, it does not reach the parties’ respective arguments concerning a duty based on the FTC Act.

breach, they have plausibly alleged a “causal nexus” between the PII that was exposed and the injuries they suffered. *Tate*, 2023 WL 6383467, at *7.

Finally, consider the economic loss doctrine. That doctrine reflects this basic rule: “where a plaintiff has suffered only economic harm as a result of a defendant’s breach of duty, the economic-loss rule will bar the tort claim if the duty arose only by contract.” *Mulch Mfg. Inc. v. Advanced Polymer Sols., LLC*, 947 F. Supp. 2d 841, 856 (S.D. Ohio 2013) (quoting *Campbell v. Krupp*, 961 N.E.2d 205, 211 (Ohio Ct. App. 2011)). In other words, “[i]f a contract imposes the duty, the loss is not compensable [under tort law]; [but] if the common law [imposes the duty], then the injury is compensable in tort.” *Tate*, 2023 WL 6383467, at *7 (citing *Chemtrol Adhesives, Inc. v. Mfrs. Mut. Ins. Co.*, 537 N.E.2d 624, 630–31 (Ohio 1989)). The Court already determined that Plaintiffs plausibly alleged a common-law duty of reasonable care to protect their PII from misuse. In other words, because Plaintiffs rely at least in part on a duty that arises under common law (as opposed to a contract), the economic loss rule does not bar Plaintiffs’ negligence claim. *Allen v. Wenco Mgmt., LLC*, 696 F. Supp. 3d 432, 439 (N.D. Ohio 2023).

2. Breach of Contract

That said, Plaintiffs also include a separate claim for breach of contract, to which the Court turns now. Under Ohio law, a contract, whether express or implied,⁸

⁸ The Court uses the term “implied contract” above to refer to an implied-in-fact contract. An implied-in-fact contract differs from an implied-in-law contract. The former refers to situations in which the factual context shows that there is an actual contract between the parties. Unlike an implied-in-fact contract, an implied-in-law contract is not a contract at all. Rather, it is a form of substantive restitution law designed to prevent unjust enrichment.

requires the same basic elements: offer, acceptance, consideration, and a meeting of the minds. *Deffren v. Johnson*, 169 N.E.3d 270, 277 (Ohio Ct. App. 2021). The only difference between an express contract and an implied contract is how to prove those elements. For an express contract, “assent to the contract[']s terms is formally expressed in the offer and acceptance of the parties.” *Realì Giampetro & Scott v. Soc’y Nat’l Bank*, 729 N.E.2d 1259, 1263 (Ohio Ct. App. 1999). When it comes to an implied contract, by contrast, “no express agreement exists.” *Id.* So the meeting of the minds is established by surrounding circumstances and tacit understanding. *Id.* Plaintiffs here allege the existence of both an express contract and an implied contract, so the Court must address each.

a. Express Contract

To demonstrate an express data security agreement between the parties, Plaintiffs point to Bon Secours’ compliance program (as expressed on its website) and its Code of Conduct. (Doc. 13, #132–33). They add that Bon Secours’ “representations ... relating to compliance with the FTC Act[and] industry practices” further evidence an express agreement. (*Id.* at #132).

Plaintiffs’ trouble, though, is that neither the compliance program nor the Code of Conduct are “contractual in nature.” *See Tucker v. Marietta Area Health Care, Inc.*, No. 2:22-cv-184, 2023 WL 423504, at *5 (S.D. Ohio Jan. 26, 2023) (rejecting the parties’ Notice of Privacy Policy as an express contract). As the name suggests, Bon

Spectrum Benefit Options, Inc. v. Med. Mut. of Ohio, 880 N.E.2d 926, 934 (Ohio Ct. App. 2007). Plaintiffs here are alleging an implied-in-fact contract.

Secours' compliance program is a *program* that attempts to “address and mitigate risks associated with an integrated global health care delivery system.” *Compliance*, Bon Secours Mercy Health (last visited May 15, 2025), <https://perma.cc/AA2T-LUYM>. In other words, it's a compliance tool, not a contract based on consideration of any kind. *Cf. Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (“[B]road statements of company policy do not generally give rise to contract claims.”). The Code of Conduct is likewise “not a bargained-for exchange of promises.” *Newman v. Howard Univ. Sch. of L.*, 715 F. Supp. 3d 86, 103 (D.D.C. 2024) (quotation omitted). It lists various rights that associates have as well as various obligations associates have. *Code of Conduct*, Bon Secours Mercy Health, <https://perma.cc/TU44-DSK3>. But it nowhere “suggests that these rights and obligations are reciprocally contingent.” *Newman*, 715 F. Supp. 3d at 103; *Clayton v. Cleveland Clinic Found.*, 2015-Ohio-1547, ¶ 11 (8th Dist.) (“Absent mutual assent[,] a handbook becomes merely a unilateral statement of rules and policies which create no obligation and rights.” (cleaned up)).⁹ Plaintiffs' breach of express contract claim thus fails.

⁹ Because the Court finds that the Code of Conduct—which is the source to which Plaintiffs point as incorporating the FTC Act's statutory obligations, (Doc. 18, #229–30 (citing Doc. 13, ¶ 179, #132–33))—is not an express contract, the Court does not reach Plaintiffs' FTC Act-related argument. Though the Court does note that “[t]he FTC[Act] does not provide a private right of action.” *Edoho-Eket v. Wayfair.com*, No. 17-6509, 2019 WL 2524366, at *2 (6th Cir. Jan. 23, 2019). So the Court seriously doubts that Plaintiffs can rely on the FTC Act, even indirectly, as the basis for their contract claim. *See Tucker*, 2023 WL 423504, at *5 (“[T]o hold otherwise would be to create a private, statutory cause of action where none exists.”).

b. Implied Contract

Plaintiffs alternatively assert an implied contract claim. They allege that, to receive employment, they had to turn over their PII to Bon Secours. (Doc. 13, #134). And through that “course of conduct,” Bon Secours implicitly agreed to adequately protect the PII. (*Id.*). Plaintiffs highlight Bon Secours’ “representations ... legal obligations, and acceptance” of Plaintiffs’ PII as evidence of the implied contract. (*Id.*).

“[I]t is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient’s assent to protect the information sufficiently.” *Castillo v. Seagate Tech., LLC*, No. 16-cv-1958, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016). In line with that observation, numerous courts have found an implied contract exists where a plaintiff alleges that she was required to turn over PII to obtain employment or a type of service. *See, e.g., Haney*, 747 F. Supp. 3d at 1113; *Brooks v. Peoples Bank*, 732 F. Supp. 3d 765, 780 (S.D. Ohio 2024); *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 821 (E.D. Ky. 2019). And that’s just what Plaintiffs allege here—that they “were required to provide Defendant with their [PII] in order to receive employment,” and that Bon Secours, in turn, impliedly “agreed to comply with its statutory and common law duties to protect their [PII].” (Doc. 13, #134). That implied agreement is even more plausible given Plaintiffs’ allegations that Bon Secours was aware of its data protection and compliance duties, as evidenced by its website and Code of Conduct. (*Id.*). All told, the Court concludes Plaintiffs have sufficiently alleged an implied-in-fact contract.

3. Unjust Enrichment

Under Ohio law, to assert an unjust enrichment claim, the plaintiff must plausibly allege: (1) that she conferred a benefit upon the defendant, (2) the defendant knew about the benefit, and (3) it would be unjust for the defendant to retain the benefit without payment. *Padula v. Wagner*, 37 N.E.3d 799, 813 (Ohio Ct. App. 2015).

Plaintiffs insist that they have conferred a monetary benefit on Bon Secours through their “labor and services” and PII. (Doc. 13, #135). And they say that Bon Secours, knowing of those benefits, enriched itself in two ways. First, Plaintiffs complain that Bon Secours enriched itself through the inherent value of Plaintiffs’ PII, which it uses to operate its business and generate revenue. (*Id.* at #135–36). Second, Plaintiffs argue that Bon Secours enriched itself by saving the costs it should have expended on data security measures. (*Id.* at #135). Neither argument works.

The first theory fails because “Plaintiffs’ personal information does not confer a benefit” upon Bon Secours. *Haney*, 747 F. Supp. 3d at 1113–14 (collecting cases). Beyond that, Plaintiffs have alleged no facts suggesting that Bon Secours “commoditized, gained monetary benefit, or otherwise profited from Plaintiffs’ PII.” *Cahill v. Mem’l Heart Inst., LLC*, No. 1:23-cv-168, 2024 WL 4311648, at *13 (E.D. Tenn. Sept. 26, 2024).

The second theory fares no better. Plaintiffs allege that they provided Bon Secours “their labor and [PII] on the understanding” that Bon Secours would pay for reasonable data privacy and security. (Doc. 13, #135). As explained, Plaintiffs’ PII did not confer a benefit on Bon Secours. So that leaves their labor. The problem, though,

is that Plaintiffs exchanged their labor with Bon Secours according to the terms of their employment agreements with the company. Thus, their claim, if they have one, is not for unjust enrichment, but rather for breach of the express or implied terms of that employment arrangement. Indeed, as noted, Plaintiffs are already pressing an implied contract claim. So that claim, not a claim for unjust enrichment, will provide the source of any rights that they have. In other words, even accepting that Plaintiffs supplied their labor and PII with “the understanding that Bon Secours “would pay ... [for] reasonable data privacy and security practices,” (*id.*), the source of that understanding arose from the terms (express or implied) of their employment agreement. And in that sense, “there was no unaccounted-for benefit to form the basis of the alleged unjust enrichment.” *Cahill*, 2024 WL 4311648, at *13.


CONCLUSION

For the reasons explained, the Court **GRANTS IN PART** and **DENIES IN PART** Bon Secours’ Motion to Dismiss (Doc. 17). The motion is **DENIED** with respect to Bon Secours’ 12(b)(1) ground seeking to dismiss for lack of jurisdiction as to Plaintiffs’ damages claims and part of the injunctive relief Plaintiffs seek, and **DENIED** with respect to Bon Secours’ 12(b)(6) ground seeking to dismiss Plaintiffs’ negligence claim and breach of implied contract claim. The motion is **GRANTED** as to Plaintiffs’ remaining claims, and the Court **DISMISSES** those claims, but **WITHOUT PREJUDICE**.

SO ORDERED.

July 2, 2025

DATE



DOUGLAS R. COLE
UNITED STATES DISTRICT JUDGE